CLAIMS

What is claimed is:

1.   A method of creating a report having security based on content of data contained in the report, the method comprising:

      retrieving a data row having data to be contained in the report;

      determining whether data in the data row will cause a data break;

      forming a first security tag if the data row causes a data break;

      associating the first security tag with a new page in the report wherein the data row is placed on the new page; and

      placing subsequent data rows on pages having the first security tag until a second security tag is formed such that data in the report is organized based on a plurality of security tags.

2.   A method as recited in claim 1 wherein the report is generated from one executable component.

3.   A method as recited in claim 1 wherein forming a first security tag further comprises:

      retrieving a security identifier for each data break wherein each data break is associated with one or more security identifiers; and

      combining the one or more security identifiers thereby creating a security tag.

4.   A method as recited in claim 3 wherein associating the first security tag with a new page in the report further comprises:

      associating a role adopted from a security system with a data row;

      mapping security identifiers in the security tag with one or more roles adopted from the security system thereby creating a security tag adaptable by the security system; and

      · associating the security tag adaptable by the security system to a page in the report.

5.   A method as recited in claim 4 wherein the security system has a plurality of roles and a plurality of users.

6.   A method as recited in claim 4 wherein mapping security identifiers in the security tag with one or more roles further comprises:

identifying a data column in the retrieved data row upon which a data break is based; and

identifying one or more roles in the security system that correspond to the data column.

7   A method as recited in claim 6 further comprising deriving translation rules to map the one or more roles in the security system with the data column.

8.   A method as recited in claim 1 further comprising:

retrieving the data from a data source; and

sorting the data from the data source based on one or more data breaks wherein a data break is caused by a change in category of data.

9.   A method as recited in claim 8 wherein a data break is a level break in the data.

10.   A method as recited in claim 1 further comprising:

determining a first role in a security system that corresponds directly to the user;

determining one or more secondary roles that correspond indirectly to the user; and

combining the first role with the one or more secondary roles thereby creating a security clearance for the user.

11.   A method as recited in claim 10 further comprising:

comparing the security clearance with a security tag to derive a subset of pages in the report that can be viewed by the user.

12.   A method of viewing a report having a security tag associated with pages in the report such that a user can only view data authorized to be shown to the user, the method comprising:

retrieving a report having a superset of pages, a page from the superset of pages having a security tag;

obtaining a list of security identifiers associated with the user;

comparing the list of security identifiers with a plurality of security

5   tags associated with the report; and

deriving a subset of pages from the superset of pages based on the comparison such that the subset of pages only contains data that the user is authorized to view.

10   13.   A method as recited in claim 12 further comprising presenting the subset of pages as a report to the user.

14.   A method as recited in claim 13 further comprising renumbering pages in the subset of pages such that the first page in the subset of pages is page one

15   and subsequent pages are renumbered consecutively.

15   A method as recited in claim 14 wherein renumbering pages in the subset of pages further comprises:

creating a first page map having a first plurality of complete cells for

20   the superset of pages wherein a complete cell represents a page;

determining whether a cell from the first plurality of complete cells represents a page the user is authorized to view; and

creating a second page map having a second plurality of partial cells wherein a partial cell represents a viewable page.

25

16.   A method as recited in claim 15 wherein creating a first page map further comprises:

comparing the list of security identifiers associated with the user with a plurality of security tags associated with the report; and

30   associating a value with each complete cell based on whether the user can view a particular page.

17   A method as recited in claim 15 wherein determining whether a cell from the first plurality of complete cells represents a page further comprises:

35   examining the content of a cell.

18.   A method as recited in claim 15 wherein creating a second page map further comprises:

        creating a partial page map cell that corresponds to a complete cell representing a page in the report; and

        inserting a first page map index value corresponding to the complete cell into the partial cell.

19.   A method as recited in claim 15 further comprising:

        inserting a second page map index value into a complete cell corresponding to a particular page the user is authorized to view.

20.   A method as recited in claim 15 further comprising:

        inserting a partial page number from the first page map into a page number component in a page in the report.

21.   A method as recited in claim 12 further comprising mapping level break identifiers in the security tag with security identifiers in the list of security identifiers associated with the user.

22.   A method as recited in claim 21 wherein comparing the list of security identifiers further comprises comparing the level break identifiers in a security tag with the security identifiers in the list of security identifiers associated with the user.

23.   A method as recited in claim 12 wherein the list of security identifiers is derived from a security system.

24.   A method as recited in claim 12 wherein deriving a subset of pages from the superset of pages further comprises:

        determining a commonality between the security tag and the list of security identifiers; and

        including a page in the subset of pages if the security tag and the list of security identifiers pass the threshold level of commonality when compared.

25. A method as recited in claim 24 wherein the threshold level of commonality is having one term in the security tag and the list of security identifiers in common.

5   26.   A method as recited in claim 12 further comprising deriving content information including page numbers related to the subset of pages.

27.   A method as recited in claim 26 wherein the content information only contains information related to the subset of pages and generally reflects a
10   level break structure of the subset of pages.

28.   A computer-readable medium containing programmed instructions arranged to generate a report having security based on content of data contained in the report in a computer system, the computer-readable medium
15   including programmed instructions for:

retrieving a data row having data to be contained in the report;
determining whether data in the data row will cause a data break;
forming a first security tag if the data row causes a data break;
associating the first security tag with a new page in the report wherein
20   the data row is placed on the new page; and

placing subsequent data rows on pages having the first security tag
until a second security tag is formed such that data in the report is presented
based on a plurality of security tags.

25   29.   A computer-readable medium as recited in claim 28, wherein the programmed instructions for forming a first security tag further comprises programmed instructions for:

retrieving a security identifier for each data break wherein each data
break contains one or more security identifiers; and
30   combining the one or more security identifiers thereby creating a
security tag.

30.   A computer-readable medium as recited in claim 28, wherein the programmed instructions for associating the first security tag with a new page
35   in the report further comprises:

associating a role adopted from a security system with a data row;

mapping security identifiers in the security tag with one or more roles adopted from the security system thereby creating a security tag adaptable by the security system; and

associating the security tag adaptable by the security system to a page

5   in the report.

31.   A computer-readable medium as recited in claim 28, wherein the programmed instructions for mapping security identifiers in the security tag with one or more roles further comprises:

10   identifying a data column in the retrieved data row upon which a data break is based; and

identifying one or more roles in the security system that correspond to the data column.

15   32.   A computer-readable medium containing programmed instructions arranged to view a report having a security tag associated with pages in the report such that a user can only view data authorized to be shown to the user, the computer-readable medium including programmed instructions for:

retrieving a report having a superset of pages, a page from the superset

20   of pages having a security tag;

obtaining a list of security identifiers associated with the user;

comparing the list of security identifiers with a plurality of security tags associated with the report; and

deriving a subset of pages from the superset of pages based on the

25   comparison such that the subset of pages only contains data that the user is authorized to view.

33.   A computer-readable medium as recited in claim 32, wherein the programmed instructions for renumbering pages in the subset of pages further

30   comprises:

creating a first page map having a first plurality of complete cells for the superset of pages wherein a complete cell represents a page;

determining whether a cell from the first plurality of complete cells represents a page the user is authorized to view; and

35   creating a second page map having a second plurality of partial cells wherein a partial cell represents a viewable page.

34. A computer-readable medium as recited in claim 32, wherein the programmed instructions for creating a first page map further comprises:

comparing the list of security identifiers associated with the user with a

5 plurality of security tags associated with the report; and

associating a value with each complete cell based on whether the user can view a particular page.

ADD A2